IN THE CLAIMS

Please amend the claims as follows:

Claim 1 (Currently Amended): An encryption algorithm management system, comprising:

a terminal unit; and

a center unit,

the terminal unit and the center unit having a common cipher-key,

said terminal unit comprising:

a transmitter configured to transmit a demand to said center unit for obtaining an encrypted data needed for decrypting a ciphered encryption algorithm, ~~and~~

an encryption controller configured to renew said common cipher-key in case of receiving said encrypted data from said center unit in response to said demand, decrypt a cipher-key for the ciphered encryption algorithm from the encrypted data with the renewed common cipher-key, and decrypt an encryption algorithm from the ciphered encryption algorithm with the cipher-key for the ciphered encryption algorithm, and

an encryption unit configured to encrypt a message with the encryption algorithm and send the encrypted message to a second terminal;

said center unit comprising:

a key controller configured to renew said common cipher-key so as to be identical with said renewed common cipher-key in case of receiving said demand from said transmitter, and

an encoder configured to produce said encrypted data by encrypting the cipher-key for the ciphered encryption algorithm with said renewed common cipher-key and transmit said encrypted data to said terminal unit.

Claims 2-3 (Canceled).

Claim 4 (Currently Amended): A terminal unit having a common cipher-key in common with a common cipher-key in a center unit, said terminal unit comprising:

a transmitter configured to transmit a demand to said center unit for obtaining an encrypted data needed for decrypting a ciphered encryption algorithm, ~~and~~

an encryption controller configured to renew said common cipher-key in case of receiving said encrypted data from said center unit in response to said demand, decrypt a cipher-key for the ciphered encryption algorithm from the encrypted data with the renewed common cipher-key, and decrypt an encryption algorithm from the ciphered encryption algorithm with the cipher-key for the ciphered encryption algorithm; and

an encryption unit configured to encrypt a message with the encryption algorithm and send the encrypted message to a second terminal.

Claim 5 (Canceled).

Claim 6 (Previously Presented): The terminal unit as recited in claim 4, wherein said encryption controller is stored in a memory area that may not be read or rewritten by outsiders.

Claims 7-13 (Canceled).

Claim 14 (Previously Presented): The system of claim 1, wherein said terminal unit further comprises an encryption algorithm memory configured to store said ciphered encryption algorithm.

Claim 15 (Canceled).

Claim 16 (Previously Presented): The system of claim 1, wherein said transmitter is further configured to transmit a demand when the encryption algorithm is decrypted.

Claim 17 (Previously Presented): The system of claim 1, wherein said transmitter is further configured to transmit a demand every predetermined number of times that the encryption algorithm is decrypted.

Claim 18 (Previously Presented): The system of claim 1, wherein said encryption controller is stored in a memory area that may not be read or rewritten by outsiders.

Claim 19 (Previously Presented): The system of claim 1, wherein said center unit further comprises a verification controller configured to determine if said terminal unit is authorized to use said encryption algorithm at the time of receiving said demand from said terminal unit, and to have said key controller renew said common cipher-key only if said terminal unit is determined to be authorized.

Claim 20 (Previously Presented): The terminal unit of claim 4, further comprising an encryption algorithm memory configured to store said ciphered encryption algorithm.

Claim 21 (Previously Presented): The terminal unit of claim 4, further comprising an encryption unit configured to encrypt a message with the encryption algorithm and send the encrypted message to a second terminal.

Claim 22 (Previously Presented): The terminal unit of claim 4, wherein said transmitter is further configured to transmit a demand when the encryption algorithm is decrypted.

Claim 23 (Previously Presented): The terminal unit of claim 4, wherein said transmitter is further configured to transmit a demand every predetermined number of times that the encryption algorithm is decrypted.

Claim 24 (Currently Amended): An encryption algorithm management system, comprising:

a terminal unit; and

a center unit,

the terminal unit and the center unit having a common cipher-key,

said terminal unit comprising:

a transmitter configured to transmit a demand to said center unit for obtaining a ciphered encryption algorithm, ~~and~~

an encryption controller configured to renew said common cipher-key in case of receiving said ciphered encryption algorithm from said center unit in response to said demand, and decrypt an encryption algorithm from the ciphered encryption algorithm with the renewed common cipher-key, and

an encryption unit configured to encrypt a message with the encryption algorithm and send the encrypted message to a second terminal;

said center unit comprising:

a key controller configured to renew said common cipher-key so as to be identical with said renewed common cipher-key in case of receiving said demand from said transmitter, and

an encoder configured to produce said ciphered encryption algorithm with said renewed common cipher-key and transmit said ciphered encrypted algorithm to said terminal unit.

Claim 25 (Previously Presented): The system of claim 24, wherein said terminal unit further comprises an encryption algorithm memory configured to store said ciphered encryption algorithm.

Claim 26 (Canceled).

Claim 27 (Previously Presented): The system of claim 24, wherein said transmitter is further configured to transmit a demand when the encryption algorithm is decrypted.

Claim 28 (Previously Presented): The system of claim 24, wherein said transmitter is further configured to transmit a demand every predetermined number of times that the encryption algorithm is decrypted.

Claim 29 (Previously Presented): The system of claim 24, wherein said encryption controller is stored in a memory area that may not be read or rewritten by outsiders.

Claim 30 (Previously Presented): The system of claim 24, wherein said center unit further comprises a verification controller configured to determine if said terminal unit is authorized to use said encryption algorithm at the time of receiving said demand from said terminal unit, and to have said key controller renew said common cipher-key only if said terminal unit is determined to be authorized.

Claim 31 (Currently Amended): A terminal unit having a common cipher-key in common with a common cipher-key in a center unit, said terminal unit comprising:

a transmitter configured to transmit a demand to said center unit for obtaining a ciphered encryption algorithm, ~~and~~

an encryption controller configured to renew said common cipher-key in case of receiving said ciphered encryption algorithm from said center unit in response to said demand, and decrypt an encryption algorithm from the ciphered encryption algorithm with the renewed common cipher-key, and

an encryption unit configured to encrypt a message with the encryption algorithm and send the encrypted message to a second terminal.

Claim 32 (Previously Presented): The terminal unit of claim 31, further comprising an encryption algorithm memory configured to store said ciphered encryption algorithm.

Claim 33 (Canceled).

Claim 34 (Previously Presented): The terminal unit of claim 31, wherein said transmitter is further configured to transmit a demand when the encryption algorithm is decrypted.

Claim 35 (Previously Presented): The terminal unit of claim 31, wherein said transmitter is further configured to transmit a demand every predetermined number of times that the encryption algorithm is decrypted.

Claim 36 (Previously Presented): The terminal unit of claim 31, wherein said encryption controller is stored in a memory area that may not be read or rewritten by outsiders.

Claims 37-38 (Canceled).

Claim 39 (Currently Amended): An encryption algorithm management system having a terminal unit and a center unit that have a common cipher-key to a ciphered encryption algorithm,

said terminal unit comprises:

a transmitter configured to transmit a demand to said center unit for obtaining an encrypted data needed for decrypting said ciphered encryption algorithm when said ciphered encryption algorithm is decrypted; ~~and~~

an encryption controller configured to renew said common cipher-key in case of receiving said encrypted data from said center unit in response to said demand, and to produce an encryption algorithm by decrypting said encrypted data with the renewed common cipher-key,

wherein said encryption controller has a counter for counting a number transmitted from a controller, and if said counter receives a number transmitted from said controller more than a prescribed number of times, said encryption controller does not produce an encryption algorithm by decrypting said encrypted data with said renewed common cipher-key, and

an encryption unit configured to encrypt a message with the encryption algorithm and send the encrypted message to a second terminal;

said center unit comprises:

a key controller configured to renew said common cipher-key so as to be identical with said renewed common cipher-key in case of receiving said demand from said transmitter; and

an encoder configured to produce said encrypted data by encrypting a cipher-key with said renewed common cipher-key and to transmit said encrypted data to said terminal unit.